LAWFARE

CYBERSECURITY AND DETERRENCE

U.S. Cyber Command and the Russian Grid: Proportional Countermeasures, Statutory Authorities and Presidential Notification

By **Robert Chesney** Monday, June 17, 2019, 4:00 PM

The New York Times published a remarkable article from David Sanger and Nicole Perlroth on Saturday, titled "U.S. Escalates Online Attacks on Russian Power Grid." To be clear, the lights are not currently flickering in Moscow. The thrust of the story, instead, is that U.S. Cyber Command (CYBERCOM) has established the ability to disrupt the operations of at least some parts of the Russian grid, in response to ongoing efforts by the Russians to do the same to us.

The article is rich with insights into the rapidly evolving state of U.S. cyber capabilities, while yielding several important questions. Below, I explore what it signifies in terms of international law and countermeasures, CYBERCOM's affirmative authority to take such actions under last year's National Defense Authorization Act (NDAA), and the legal and policy issues when it comes to notifying the president of such operations.

1. Crossing the Rubicon or a Proportional Countermeasure?

Some of the commentary excited by this article has expressed concern that the United States is crossing a Rubicon here, breaching a valuable taboo. These U.S. actions, however, are occurring in response to *years* of Russian efforts to establish just this sort of access to U.S. energy systems. From the article:

At the end of Mr. Obama's first term, government officials began uncovering a Russian hacking group, alternately known to private security researchers as Energetic Bear or Dragonfly. But the assumption was that the Russians were conducting surveillance, and would stop well short of actual disruption. That assumption evaporated in 2014, two former officials said, when the same Russian hacking outfit compromised the software updates that reached into hundreds of systems that have access to the power switches …

In December 2015, a Russian intelligence unit shut off power to hundreds of thousands of people in western Ukraine. The attack lasted only a few hours, but it was enough to sound alarms at the White House. A team of American experts was dispatched to examine the damage, and concluded that one of the same Russian intelligence units that wreaked havoc in Ukraine had made significant inroads into the United States energy grid …

In late 2015 … yet another Russian hacking unit began targeting critical American infrastructure, including the electricity grid and nuclear power plants. By 2016, the hackers were scrutinizing the systems that control the power switches at the plants …

[In 2018 CYBERCOM's] staff was assessing Russian hackings on targets that included the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., as well as previously unreported attempts to infiltrate Nebraska Public Power District's Cooper Nuclear Station, near Brownville. The hackers got into communications networks, but never took over control systems …

In the past few months … energy companies in the United States and oil and gas operators across North America discovered their networks had been examined by the same Russian hackers who successfully dismantled the safety systems in 2017 at Petro Rabigh, a Saudi petrochemical plant and oil refinery.

Does that mean there is no cause for concern here?

From a policy perspective, one might argue that a U.S. decision to take certain legal and policy positions will have a trailblazing influence on others that a comparable Russian decision does not. That is a very hard claim to justify vis-a-vis decision-making in China, Iran and North Korea, however, and it's not clear how much bite it has elsewhere (though we have often seen arguments of this kind in the context of drones, demonstrating that the claim has an intuitive appeal to many).

From an international law perspective, one might argue that compromising the grid is an internationally wrongful act. If so, however, the context suggests that the CYBERCOM activity may constitute a lawful countermeasure, given the earlier Russian intrusions to U.S. systems. Here is Prof. Mike Schmitt's thumbnail sketch of countermeasures:

Because they involve an act that would otherwise be unlawful, countermeasures are subject to strict conditions. Several merit mention. First, countermeasure may not be conducted until the injured state has notified the responsible state that it intends to take countermeasures and gives the responsible state an opportunity to desist in its unlawful conduct. In the cyber context, it is important to point out that the notification requirement is subject to a condition of feasibility, for advance notification that a cyber countermeasure is about to be taken may afford the responsible state the opportunity to foil it. Second, countermeasures must be proportionate to the injury to which they respond. In particular, they have to be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the right question." Third, treaties may contain provisions for the taking of specified remedies in the event of breach. If so, the injured state must resort to them before taking countermeasures.

While we do not truly have enough information in the public record to pass a reliable judgment on the matter, we can at least say that there is a plausible case here for categorizing the CYBERCOM action as a countermeasure responding proportionally to Russia's activities in U.S. energy systems.

2. Illustrating the Impact of the Recent Expansion of CYBERCOM's Statutory Authorities

A second key feature of the story is its emphasis on the evolving domestic law architecture for CYBERCOM's external operations. The article notes that "the action inside the Russian electric grid appears to have been conducted under little-noticed new legal authorities, slipped into the military authorization bill passed by Congress last summer."

If those authorities really were little-noticed, it wasn't for lack of effort here at Lawfare. I wrote an extensive analysis of them here pre-enactment (and also here, in order to explain how they relate to CYBERCOM's "defend forward" operational concept). In relevant part, here is how I described Section 1642 of the NDAA, which the article suggests may have provided the affirmative authority upon which CYBERCOM relied to conduct its Russian grid ops:

[Section 1642] is not styled as an "Authorization for Use of Military Force" (AUMF), and it certainly is not an authorization to do anything militarily involving *non*-cyber means. And yet it is an AUMF of a very narrow and specific variety. It authorizes action of the following kind and subject to the following conditions, when the executive branch finds that those conditions are satisfied and decides to invoke this grant of authority…

Two elements must be satisfied in order to trigger this authorization:

> (1) There must be "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes";
>
> (2) The responsible party must be Russia, China, North Korea or Iran.

Note that Section 1642 makes the "National Command Authority" the relevant decision maker on those triggers. The NCA is, of course, the president together with the secretary of defense. Very interesting to specify the NCA as opposed to just the president, no?

Once those determinations are made by the NCA, Section 1642 pre-authorizes CYBERCOM in particular "to take appropriate and **proportional** action in foreign cyberspace to disrupt, defeat, and deter such attacks" (emphasis added by me). And the statute goes on to emphasize that this will count as "traditional military activity," thus reinforcing Section 1632's attempt to put an end to Title 50-related objections to CYBERCOM operations. …

This maps onto the reported CYBERCOM operations in the Russian grid quite well, bearing in mind that Russian activities in *our* energy systems plausibly qualify as an "active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace" conducted by a state on the qualifying list.

This leads us to the next question, about which the article also shares some fascinating details: Must the president be in the loop for such significant operations?

3. POTUS Out of the Loop—Bugs and Features

This may come as a shock to those who don't follow this area closely, but under the NDAA framework and especially the relevant National Security Presidential Memorandum (NSPM-13), it does not appear that presidential authorization was required for this activity.

First, the NDAA system: In addition to confirming CYBERCOM's authority to engage in proportional responses to this sort of attack (see the Section 1642 analysis above), the NDAA also contains a complex set of provisions intended to ensure that these sorts of operations do not wind up categorized as "covert action" subject to the panoply of Title 50 rules—including signed presidential

findings—that normally come into play when the government conducts operations where the sponsoring role of the United States is not meant to be apparent or acknowledged. Simply put, Section 1632 of the NDAA establishes that such activities instead constitute Title 10 "traditional military activities." (See here for my detailed explanation in 2018.)

Second, the Trump administration last year expressly modified internal executive branch rules that previously ensured presidential sign-off on out-of-network CYBERCOM activities, in an effort to push decision-making authority for most such operations outside the White House. The details of NSPM-13 remain classified, but extensive public statements have confirmed that much (see Ellen Nakashima's article here, for example).

The legally interesting question here, then, is whether this particular set of operations fits within the NSPM-13 thresholds. Without access to the precise language, we can't judge it from the outside. That said, according to a passage in Nakashima's 2018 reporting on NSPM-13, presidential involvement is still required when the operation "would cause death, destruction, or significant economic impacts":

In general, the president's directive—called National Security Presidential Memorandum 13, or NSPM 13—frees the military to engage, without a lengthy approval process, in actions that fall below the "use of force" or a level that would cause death, destruction or significant economic impacts, said individuals familiar with the policy who spoke on the condition of anonymity to discuss nonpublic information.

At first blush, one might think that an operation establishing the capability to compromise some or all of a country's grid might satisfy that test. The fact that it apparently did not probably indicates that the test is understood to be triggered only when such operational effects are put into play, and not at the preparation of the battlefield stage in which the capability to cause such effects is being established in the first place (though it might also be a clue that the hacks at issue are much narrower in scope and capability than the general framing of the Times story suggests).

At any rate, let's assume that this is the right conclusion. It is a *very* interesting question whether that is the right place to draw the line for ensuring presidential engagement. In an ordinary presidential administration, one might be inclined to argue that the line instead should be drawn at the point where the operation creates the capability to cause such effects, even if no one currently plans to put that capability into practice. But these are not ordinary times, as the Times article underscores.

Here's the most remarkable passage in the Times article:

Two administration officials said they believed Mr. Trump had not been briefed in any detail .... Pentagon and intelligence officials described broad hesitation to go into detail with Mr. Trump about operations against Russia for concern over his reaction — and the possibility that he might countermand it or discuss it with foreign officials .... Because the new law defines the actions in cyberspace as akin to traditional military activity on the ground, in the air or at sea, no such briefing would be necessary, they added.

They were right that it was not legally required. And I think they were right to be concerned about the possible consequences of elevating this to the president's attention. And yet it is quite unsettling, from the perspective of civil-military relations in general (and deep, important traditions regarding civilian control of the military in particular) to see such a stark illustration of where things stand.

Topics: Cybersecurity and Deterrence

Tags: Cybersecurity, Russia, CYBERCOM, Cybercommand, Cyber Command

Bobby Chesney is the **Charles I. Francis Professor in Law** and Associate Dean for Academic Affairs at the University of Texas School of Law. He also serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law. His scholarship encompasses a wide range of issues relating to national security and the law, including detention, targeting, prosecution, covert action, and the state secrets privilege; most of it is posted **here**. Along with Ben Wittes and Jack Goldsmith, he is one of the co-founders of the blog.

@bobbychesney